

United States Senate

WASHINGTON, DC 20510

February 7, 2019

Mr. Mark Zuckerberg
Chief Executive Officer
Facebook
1 Hacker Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg,

We write concerned about reports that Facebook is collecting highly-sensitive data on teenagers, including their web browsing, phone use, communications, and locations – all to profile their behavior without adequate disclosure, consent, or oversight. These reports fit with longstanding concerns that Facebook has used its products to deeply intrude into personal privacy. Additionally, the scope of the research and the use of the Onavo Protect app raises questions about Facebook's use of personal data to engage in potentially anti-competitive behavior. We write to request information about how Facebook conducted its Project Atlas program and how it used sensitive data collected from participants.

On January 29, 2019, TechCrunch reported that Facebook has run a paid research program named Project Atlas to profile consumers by monitoring their phone use. According to registration pages and advertisements run by Facebook's research partners, the program was available to individuals between the ages of 13 and 35, requiring parental consent for those younger than 18. Despite this constraint, the program appears to have specifically targeted teens, inadequately disclosed the scope of the data collection, and not properly verified parental consent. One advertisement for the program on Snapchat and Instagram found by TechCrunch shows a teen with hundred dollar bills falling from the sky, calling for "participants for a paid social media research study." According to a journalist who attempted to register as a teen, the linked registration page failed to impose meaningful checks on parental consent.¹ Facebook has more rigorous mechanisms to obtain and verify parental consent, such as when it is required to sign up for Messenger Kids.² This recruitment and lax oversight of teen privacy flies in the face of a widespread understanding that young people require strong protections for their privacy and safety.

Facebook's monitoring under Project Atlas is particularly concerning because the data collection performed by the research app was deeply invasive. Facebook's registration process encouraged participants to "set it and forget it," warning that if a participant disconnected from

¹ Kelion, Leo. "Facebook Adviser Criticises 'lax' Child Checks." BBC News. January 31, 2019. <https://www.bbc.com/news/technology-47071334>.

² Cheng, Loren. "Introducing Messenger Kids, a New App For Families to Connect." Facebook Newsroom. December 4, 2017. <https://newsroom.fb.com/news/2017/12/introducing-messenger-kids-a-new-app-for-families-to-connect/>.

the monitoring for more than ten minutes for a few days that they could be disqualified. Behind the scenes, the app watched everything on the phone.

Once installed, the app added a VPN connection that would automatically route all of a participant's traffic through Facebook servers. The app also installed an SSL root certificate on the participant's phone, which would allow Facebook to intercept or modify data sent to encrypted websites. As a result, Facebook would have limitless access to monitor normally secure web traffic, even allowing Facebook to watch an individual log into their bank account or exchange pictures with their family. None of the disclosures provided at registration offer a meaningful explanation about how that sensitive data is used, how long it is kept, or who within Facebook has access to it. Facebook could have access to messages or images that teens and adults had sent believing they were private without any awareness or ability to control the use of this private information.

Since Facebook did its analysis on the server side of the relationship, a participant or an independent researcher has no way of knowing what Facebook was looking for or how long it stored the data. Facebook could have designed the Project Atlas app in a manner that would limit the data that was sent back to Facebook. Moreover, it could have limited the types of data captured, such as looking at domain name lookups (e.g. telling Facebook "the participant opened Gmail") rather than decrypting the content of encrypted communications (e.g. telling Facebook "the participant is sending an email to their cousin using Gmail with an attached picture of their dog."). It is unclear whether Facebook was looking for specific items of interest, or whether it was retaining all traffic that might prove interesting down the road. In recent cases involving market research programs at Sears and Lenovo, the Federal Trade Commission (FTC) found that, even when paid, such programs must fully disclose the types of data collected and purposes for monitoring, particularly when programs involve the interception of encrypted web traffic.³⁴

Lastly, Project Atlas is particularly concerning in light of Facebook's established history of using private information for potentially anti-competitive purposes. In order to monitor participants, Facebook used a version of its Onavo Protect app, a web security application that it acquired in 2013. Onavo Protect has its own history of privacy and competition concerns. According to Buzzfeed and the Wall Street Journal, Facebook has used web browsing data collected from Onavo Protect users to monitor rival products and identify emerging competitors to buy or copy. Privacy advocates have challenged that the further analysis of this sensitive browsing data is not disclosed to users.⁵ In August 2018, Apple banned Onavo Protect from the App Store for breaching its policies about transparency and limits on the data that apps are allowed to collect.

³ Federal Trade Commission, In the Matter of Sears Holdings Management Corporation, Docket No. C-0823099. <https://www.ftc.gov/sites/default/files/documents/cases/2009/06/090604searscomplaint.pdf>

⁴ Federal Trade Commission, In the Matter of Lenovo (United States) Inc. Docket No. C-1523134. https://www.ftc.gov/system/files/documents/cases/1523134_lenovo_united_states_complaint.pdf

⁵ Comments of the Electronic Privacy Information Center, Center for Digital Democracy, Consumer Federation of America, and U.S. Public Interest Research Group to the Federal Trade Commission regarding Competition and Consumer Protection in the 21st Century Hearings. August 20, 2018. <https://epic.org/apa/comments/EPIC-FTC-CompetitionHearings-August2018.pdf>

Faced with that ban, Facebook appears to have circumvented Apple's attempts to protect consumers. With Project Atlas, Facebook distributed the application to teens through an enterprise program offered by Apple meant only for Facebook's own employees. Apple has acknowledged that Facebook's use of the enterprise certificate program for installing apps on consumers' phones constituted a breach of its terms of service.

Given the sensitivity and seriousness of any intrusions into the privacy of teens, we respectfully request a written response to the following questions by March 1, 2019:

1. When did Project Atlas begin and how many individuals have participated in the program? How many of those participants were under 18?
2. Did Facebook or its partners specifically target teenagers with advertisements at any point in the research program? Did it provide referral payments targeted specifically to recruit teenagers?
3. Why did Facebook use a less strict mechanism for verifying parental consent than is required for Messenger Kids or Global Data Protection Regulation (GDPR) compliance?
4. What specific types of data was collected (e.g. device identifiers, usage of specific applications, content of messages, friends lists, location, et al.)?
5. Did Facebook use the root certificate installed on a participant device by the Project Atlas app to decrypt and inspect encrypted web traffic? Did this monitoring include analysis or retention of application-layer content?
6. For what specific purposes was the app usage or collected internet traffic used, and for how long was this data retained?
7. Were app usage data or communications content collected by Project Atlas ever reviewed by or available to Facebook personnel or employees of Facebook partners?
8. Given that Project Atlas acknowledged the collection of "data about [users'] activities and content within those apps," did Facebook ever collect or retain the private messages, photos, or other communications sent or received over non-Facebook products?
9. Did Facebook collect or retain communications sent to participants' devices in the Project Atlas program? If so, did it obtain consent to store personal data from those third parties?
10. Has Facebook ever used traffic information collected from Onavo or Project Atlas to monitor the adoption or popularity of non-Facebook products or services? Has the data from either ever informed Facebook's acquisition decisions regarding such products or services?

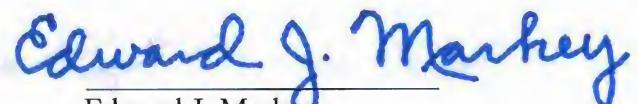
11. Why did Facebook bypass Apple's app review? Has Facebook bypassed the App Store approval processing using enterprise certificates for any other app that was used for non-internal purposes? If so, please list and describe those apps.
12. In light of recent invasions of children's and teens' privacy, including those described above, would Facebook support federal legislation to create new privacy safeguards for children and teens online?

Thank you for your attention to these important issues. We look forward to your response.

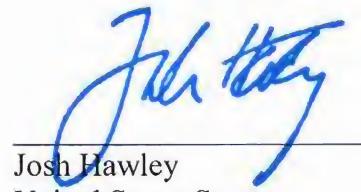
Sincerely,



Richard Blumenthal
United States Senate



Edward J. Markey
United States Senate



Josh Hawley
United States Senate